UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,082	04/19/2004	Christopher G. Kaler	13768.506	1874

22913 7590 06/20/2008

WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/827,082	KALER ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,21-30,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13, 21-30, 32 and 33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on March 26th, 2008. Claims 1, 8, 21 and 26 have been amended; Claims 1-13, 21-30, 32 and 33 are pending and have been considered below.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 26th, 2008 has been entered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 7 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 7 recites the limitation "the requesting code" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 21-30, 32 and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Traw et al. (6,542,610).

Claims 21 and 32: Traw et al. discloses a method and computer program product for authorizing the requester to interact with the provider, the method comprising:

a. sending a request to the provider*(devices exchange challenges)* [column 7, lines 6-15];

b. receiving a configuration challenge from the provider, the configuration challenge including information indicating how the requester is to prove that the requester is appropriately configured to interact with the provider*(ie. device certificates typically contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use)* [column 5, lines 1-10];

c. formulating proof, based on a measurable aspect of the requester's configuration, that the measurable aspect of the requesting computing system's configuration is appropriate for accessing a resource the measurable aspect comprising at least a region within a portion of executable instructions*(ie. formulating a response to a challenge with the appropriate key length and type of cipher as defined in the device certificate contained in the challenge)* [column 5, lines 1-10];

d. sending proof*(response)* of the values of one or more measurable aspects of the requester to the provider [column 7, lines 6-15];

e. receiving a token*(control channel key)* that can be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 22: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending a request to the provider comprises an act of sending a challenge along with the request, the challenge indicating how the provider is to prove that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 23: Traw et al. discloses a method as in claim 21 above and further discloses that the act of receiving a configuration challenge from the provider comprises an act receiving a configuration challenge along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15].

Claim 24: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending proof*(response)* of the values of one or more measurable aspects of the requester to the provider comprises an act of sending a challenge along with the proof*(response)* of the values of one or more measurable aspects, the challenge indicating how the provider is to prove that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 25: Traw et al. discloses a method as in claim 21 above and further discloses an act of receiving a token comprises an act of receiving a token*(control channel key)* along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claims 26 and 33: Traw et al. discloses a method and computer program product for authorizing the requester and the provider to interact with the provider, the method comprising:

a. an act of receiving a request from the requester*(devices exchange challenges)* [column 7, lines 6-15];

b. an act of causing a configuration challenge to be issued to the requester, the configuration challenge requesting proof that the requester is appropriately configured to interact with the provider*(devices exchange challenges)* [column 7, lines 6-15];

c. an act of receiving proof*(response)* of the values of one or more measurable aspects of the requester's configuration the one or more measurable aspects comprising at least a region within a portion of executable instructions [column 7, lines 6-15];

d. and an act of sending a token*(control channel key)* that can subsequently be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 27: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving a request comprises an act of receiving a challenge along with the request, the challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 28: Traw et al. discloses a method as in claim 26 above and further discloses that the act of causing a configuration challenge to be issued to the requester comprises an act of sending a configuration challenge along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 29: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving proof of the values of one or more measurable aspects of the requester's configuration comprises an act of receiving a challenge along with the proof*(response)* of the values of the one or more measurable aspects, the challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 30: Traw et al. discloses a method as in claim 26 above and further discloses that the act of sending a token comprises sending a token*(control channel key)* along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al. (6,542,610) in view of Benoit (6,820,814).

Claim 1: Traw et al. discloses a method for providing information that can be used to verify measurable aspects of a requesting computing system, the method comprising:

a. determining that the providing computing system*(Device A)* is appropriately configured to issue challenges to components included in the requesting computing system*(Device B)* and determining that the providing application is appropriately configured to issue challenges to the requesting instructions*(Device A sends a challenge to Device B and compares the response to an expected value)* [column 7, lines 16-41];

b. receiving a challenge initiated by the providing application based at least in part on the providing computing system and the providing application*(following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages)*, the challenge including information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource*(ie. device certificates typically contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use)* [column 8, lines 33-39 | column 5, lines 1-10];

c. formulating proof, based on a measurable aspect of the requesting computing system's configuration, that the measurable aspect of the requesting computing system's configuration is appropriate for accessing a resource*(ie. formulating a response to a challenge with the appropriate key length and type of cipher as defined in the device certificate contained in the challenge)* [column 5, lines 1-10];

d. and submitting an assertion that can be used to verify that the requesting computing system is appropriately configured to access a resource*(signed messages)* [column 8, lines 33-39].

Furthermore, Traw et al. discloses that the challenge includes information*(ie. device certificates, which are concatenated with a random challenge, provide information regarding the authentication)* identifying authentication parameters*(ie. determining what authentication level to employ and what cipher systems to use when encrypting the random challenge, etc.)* [column 5, lines 1-10 & column 8, lines 17-20], but does not explicitly disclose that the challenge includes information comprising at least the identity of a region within a portion of instructions at the requesting computing system computed from a first random value and a second random value.

Nonetheless, Benoit discloses a similar invention and further discloses a cipher system which utilizing a first and second random value to identify a particular output data from input data*(ie. calculate and obtain output)* [column 5, lines 20-34].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the invention disclosed by Traw et al. with the features disclosed by Benoit in order to further protect encrypted information, as suggested by Benoit [column 5, lines 8-15].

Claim 3: Traw et al. and Benoit disclose a method as in claim 1 above, and Traw et al. further discloses that the act of determining that the providing application is appropriately configured to issue challenges to the requesting instructions comprises receiving proof that the providing application complies with one or more security and trust policies of the requesting computing system*(compares data string to expected value to determine if devices can exchange protect content)* [column 7, lines 16-41].

Claim 4: Traw et al. and Benoit disclose a method as in claim 1 above, and Traw et al. further discloses that receiving a challenge that was initiated by the providing application comprises receiving a request for proof of

the values*(signed message)* of one or more measurable aspects of the requesting computer system*(Device B transmits signed message to Device A)* [column 8, lines 33-39]. The examiner notes that the act of transmitting a proof value to Device A implies that Device B has accepted a request for a proof value.

Claim 5: Traw et al. and Benoit disclose a method as in claim 1 above, and Traw et al. further discloses that the submitted assertion includes the values of one or more measurable aspects of the requesting computer system*(signed message contains random challenge and Diffie-Hellman key exchange value)* [column 8, lines 33-39].

Claim 6: Traw et al. and Benoit disclose a method as in claim 1 above, and Benoit further discloses that the submitted assertion indicates the identity*(ie. calculate and obtain output)* of one or more portions of the requesting instructions [column 5, lines 20-34].

Claim 7: Traw et al. and Benoit disclose a method as in claim 1 above, and Traw et al. further discloses that the submitted/received assertion indicates an execution environment*(ie. if expected value not indicates a security threat on the system)* [column 7, lines 6-15].

Claim 8: Traw et al. discloses a method for verifying measurable aspects of the requesting computing system, the method comprising:

a. proving that the providing computing system*(Device A)* is appropriately configured to issue challenges to components of the requesting computing system*(Device B) (each device verifies that the appropriate response has been received)* [column 7, lines 16-41];

b. causing a configuration challenge to be issued to the requesting instructions*(following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages)*, the challenge including information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource*(ie. device certificates typically*

contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use) [column 8, lines 33-39 | column 5, lines 1-10];

c. receiving an assertion that can be used to verify that the requesting instructions are configured appropriately for interacting with the providing application*(signed messages)*, the assertion including information based at least in part upon both a measurable aspect of the requesting system is configured and the information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured*(ie. formulating a response to a challenge with the appropriate key length and type of cipher as defined in the device certificate contained in the challenge)* [column 8, lines 33-39 | column 5, lines 1-10].

Furthermore, Traw et al. discloses that the challenge includes information*(ie. device certificates, which are concatenated with a random challenge, provide information regarding the authentication)* identifying authentication parameters*(ie. determining what authentication level to employ and what cipher systems to use when encrypting the random challenge, etc.)* [column 5, lines 1-10 & column 8, lines 17-20], but does not explicitly disclose that the challenge includes information comprising at least the identity of a region within a portion of instructions at the requesting computing system computed from a first random value and a second random value.

Nonetheless, Benoit discloses a similar invention and further discloses a cipher system which utilizing a first and second random value to identify a particular output data from input data*(ie. calculate and obtain output)* [column 5, lines 20-34].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the invention disclosed by Traw et al. with the features disclosed by Benoit in order to further protect encrypted information, as suggested by Benoit [column 5, lines 8-15].

Claim 10: Traw et al. and Benoit disclose a method as in claim 8 above, and Traw et al. further discloses that the act of proving that the providing application is appropriately configured to issue challenges to the requesting instructions comprises an act of sending proof*(data string)* that the providing application complies with one or more security and trust policies of the requesting computing system*(compares data string to expected value to determine if devices can exchange protect content)* [column 7, lines 16-41].

Claim 11: Traw et al. and Benoit disclose a method as in claim 8 above, and Traw et al. further discloses that causing a challenge to be issued to the requesting computing system comprises an act of requesting proof of the values of one or more measurable aspects of the requesting computer system*(signed message contains random challenge and Diffie-Hellman key exchange value)* [column 8, lines 33-39].

Claim 12: Traw et al. and Benoit disclose a method as in claim 8 above, and Benoit further discloses that the received assertion indicates the identity*(ie. calculate and obtain output)* of one or more portions of the requesting instructions [column 5, lines 20-34].

Claim 13: Traw et al. and Benoit disclose a method as in claim 8 above, and Traw et al. further discloses that the submitted/received assertion indicates an execution environment*(ie. if expected value not indicates a security threat on the system)* [column 7, lines 6-15].

Claims 2 and 9: Traw et al. and Benoit disclose a method as in claims 1 and 8 above, but does not explicitly disclose determining that the providing computing system is appropriately configured to issue challenges to components included in the requesting computing system comprises an act of establishing an SSL connection between the requesting computing system and the providing computer system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to employ an SSL connection or any other form of secure connection between two computers when transmitting sensitive data across a network. One would have been motivated to do so in order to increase the integrity of the system.

Response to Arguments

10. Applicant's arguments with respect to claims 1, 6, 8 and 12 have been considered but are moot in view of the new ground(s) of rejection.

11. Applicant's arguments filed March 26th, 2008 have been fully considered but they are not persuasive.

12. **Regarding Claims 21 and 26:** The Applicant argues that the Traw et al. reference fails to teach proof, based on a measurable aspect of the requester's configuration, wherein the measurable aspect(s) comprises at least a region within a portion of executable instructions. However, the Examiner respectfully disagrees and submits that Traw et al. does in fact disclose this feature. Traw et al. discloses a proof*(ie. response to challenge)* based on a measurable aspect which comprises at least a region within a portion of executable instructions*(ie. data string comprising a random challenge which is encrypted and then hashed)* [column 7, lines 16-33]. Furthermore, the Examiner respectfully notes that the limitation "a region within a portion of executable instructions" may be reasonably interpreted to encompass any region of a portion of code, as the instant claims do not appear to explicitly recite what region and/or portion is encompassed. Thus, the Examiner maintains that the "measurable aspect"*(ie. if the user can generate the correct expected value)* disclosed by Traw et al. does in fact comprise at least a region within a portion of executable instructions*(ie. a random challenge, an encrypted challenge using a baseline cipher, etc.)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
June 15, 2008
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135